UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/893,785	06/29/2001	Kenji Ohkuma	210580US2SRD	4586

22850 7590 07/14/2006

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/893,785	OHKUMA ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-6 and 8-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-6 and 8-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20060131*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 28 April 2006 has been entered.

2. By the above submission, Claims 1, 4, and 12-18 have been amended. No Claims have been added or canceled. Claims 1, 4-6, and 8-18 are currently pending in the present application.

Response to Arguments

3. Applicant's arguments filed 28 April 2006 have been fully considered but they are not persuasive.

Claims 1, 4-6, and 8-18 were rejected under 35 U.S.C. 112, second paragraph, as indefinite. Claims 1, 4-6, 8, 9, 11, and 14-18 were rejected under 35 U.S.C. 102(b) as anticipated by Delayaye et al, US Patent 4751733, and Claims 10, 12, and 13 were

rejected under 35 U.S.C. 103(a) as unpatentable over Delayaye in view of Matsui et al, US Patent 6201869.

Regarding the rejection under 35 U.S.C. 112, second paragraph, the Examiner first notes that the amendments to the claims removing the terms "with respect to a size", removing the phrase "reflected on a bit", and correcting antecedent basis issues have rendered those issues moot. Regarding the limitations of connecting "at least one input bit terminal of the first units to one bit terminal of the corresponding first unit ... via at least two paths" in, for example, Claims 1, 4, 12, 13, and 16, Applicant argues that Figure 35 shows input bit terminals 1001 and 1002 (see page 11 of the present response). The Examiner notes that this contradicts both the comments in the previous response and, more tellingly, the present specification, noting that elements 1001 and 1002 are referred to as S-boxes (see page 16 of the response received 29 August 2005 and page 53 of the present specification). The Examiner further notes that there does not appear to be written description of the limitation "input bit terminal" in the disclosure as originally filed.

Therefore, the Examiner maintains that the claimed language regarding input bit terminals appears to be inconsistent with the disclosure of the invention. As per Figure 35, an S-box ("first unit") and a succeeding S-box ("corresponding first unit in the succeeding encryption section") are interconnected by two to four paths. This is contrasted with previously known methods as depicted in Figure 36 of the present application where a first S-box is connected to a succeeding S-box by only one path. In further contrast, the claimed limitation of an "input bit terminal" being connected to a

corresponding input bit terminal by at least two paths appears to require that individual or single input bit terminals of the S-boxes are literally connected by multiple paths. The Examiner notes that the phrase "input bit terminal", lacking any further definition or clarification in the specification (indeed, lacking explicit mention at all), suggests that it is an input terminal for a single bit at a time and no more. However, it is not clear how such a single terminal can be connected to a corresponding single terminal by multiple paths and result in a single input bit for the corresponding terminal. As stated in the previous Office action, although the claim language appears to contradict what, as per Applicant's description in the specification and the previous response, the claims are intended to encompass, for the purposes of advancing the prosecution of the present application, the claims have been examined and were examined previously as though the recited the intended limitations, in anticipation of the claims being brought into compliance with 35 U.S.C. 112, first and second paragraphs (see the rejections below).

In light of the arguments above, the Examiner still believes that Delayaye does disclose that each S-box is connected to a succeeding S-box by at least two paths. The Examiner again notes that in Figure 1 of Delayaye, there are disclosed multiple substitution units, corresponding to the S-boxes, i.e. the claimed "first units", "first nonlinear transformation units", or "randomizing operations", that provide input to each permutation circuit, corresponding to the diffusion units or operations. As noted by the Applicant, examples of the permutation circuits are shown in Figures 5 and 6 of Delayaye. The Examiner again notes that each group of eight bits in those figures is output from a different substitution unit. Therefore, each substitution unit is connected

to each succeeding corresponding substitution unit by multiple paths, as shown in Figures 5 and 6.

The Examiner notes that the above arguments are based on a conventional understanding of the concept of transmitting bits between the operational units. If alternative definitions or understandings for such a concept were intended, the Examiner respectfully requests that Applicant point out in the present disclosure where such alternative definitions have been set forth.

Therefore, for the reasons detailed above, the Examiner maintains the rejections set forth below.

Information Disclosure Statement

4. The information disclosure statement filed 31 January 2006 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because each page of the information disclosure statement fails to include the three items required by 37 CFR 1.98(a)(1), namely (i) the application number of the application in which the information disclosure statement is being submitted, (ii) a column that provides a space for the examiner's initials next to each document to be considered, and (iii) a heading clearly indicating that the list is an information disclosure statement. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any

missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

Specification

5. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: the specification does not provide proper antecedent basis for the limitations in Claims 1, 4-6, 12, 13, and 16 regarding connecting "at least one input bit terminal of the first units to one input bit terminal of the corresponding first unit in the succeeding encryption section via at least two paths". In particular, the specification does not provide any antecedent basis for the phrase "input bit terminal". See below regarding the rejection under 35 U.S.C. 112, first paragraph, for failure to comply with the written description requirement.

Claim Objections

6. Claim 16 is objected to because of the following informalities:

In Claim 16, in lines 8 and 10 of the claim, it appears that "encrypting section" is intended to read "decrypting section".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 1, 4-6, 8-13, and 16 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Specifically, independent Claims 1, 4, 12, 13, and 16, along with dependent Claims 5 and 6, recite limitations such as "to connect at least one input bit terminal of the first units to one input bit terminal of the corresponding first unit in the succeeding encryption section via at least two paths" (as in Claim 1). There does not appear to be any support in the specification for explicitly connecting input bit terminals of first units to a terminal in a corresponding succeeding unit, whether by single or multiple paths. Further, the term "input bit terminal" does not appear to be mentioned in the specification whatsoever. Claims not specifically referred to are rejected due to their dependence on a rejected base claim.

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 1, 4-6, and 8-18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "a group of data which is of the first size and is output from the first units" in line 6 of the claim. It is not clear whether the group as a whole is of the first size or if the data itself is of the first size, nor is it clear whether the group as a whole is output from the first units or the data itself. Similarly, **Claim 4** recites "a group of the first subblock data which is of the first size and is output from the first nonlinear transformation units" in lines 7-9 of the claim and "a group of the second subblock data which is of the third size and is output from the second nonlinear transformation units" at lines 15-17 of the claim. It is not clear whether the group of first subblock data as a whole is of the first size, or if the first subblock data itself is of the first size; similarly, it is not clear whether the group of second subblock data as a whole is of the third size or if the second subblock data itself is of the third size. Further, **Claim 12** recites "a group of the first subblock data of 128 bits output from the four first nonlinear transformation units" in line 7 of the claim; it is not clear whether the group as a whole is 128 bits or the first subblock data within the group are each 128 bits. **Claim 12** also recites "a group of the second subblock data of 32 bits output from the second nonlinear transformation units"; similarly, **Claim 13** recites "a group of the first subblock data of 64 bits output from the two first nonlinear transformation units" and "a group of the second subblock data of 32 bits output from the second nonlinear transformation

units"; **Claim 14** recites "a group of the randomized data of the first size"; **Claim 15** recites "a group of the randomized data of the first size"; **Claim 16** recites "a group of data which is of the first size and is output from the first units"; **Claim 17** recites "a group of the randomized data of the first size"; and **Claim 18** recites "a group of the randomized data of the first size". In each of the above cases, the claims are rendered indefinite because it is not clear what the subject of the limitations regarding sizes, bit lengths, or outputting is; that is, it is not clear whether the limitations apply to the groups of data as whole units, or to the pieces of data within the groups.

Claim 1 further recites the limitation "to connect at least one input bit terminal of the first units to one input bit terminal of the corresponding first unit in the succeeding encryption section via at least two paths". This is inconsistent with the description in the specification (see page 53 and Figure 35 of the present disclosure); specifically, the disclosure states that the it is the S-boxes, corresponding to the claimed "first units", are interconnected by two to four paths. This is in contrast to the claim language, which recites that individual bit terminals of the S-boxes are literally connected by multiple paths. This contradiction renders the claim indefinite. **Claim 4** similarly recites the limitation "to connect at least one input bit terminal of the first nonlinear transformation units to one input bit terminal of the corresponding first nonlinear transformation units in the succeeding encryption section via at least two paths". **Claim 5** also recites "input bit terminals of a second non-linear transformation unit are connected to input bit terminals of a corresponding second nonlinear transformation unit in the succeeding first nonlinear transformation unit via at least two paths"; **Claim 6** recites "input bit terminals

of more than one second nonlinear transformation unit are connected to input bit terminals of corresponding second nonlinear transformation units in the succeeding first nonlinear transformation unit via at least two paths"; **Claims 12 and 13** each recite "to connect at least one input bit terminal of the first nonlinear transformation units to one input bit terminal of the corresponding first nonlinear transformation units in the succeeding encryption section via at least two paths"; and **Claim 16** recites "to connect at least one input bit terminal of the first units to one input bit terminal of the corresponding first unit in the succeeding encryption section via at least two paths". In each of the above cases, the contradiction between the claim language and the description in the disclosure renders the claims indefinite, as noted above in reference to Claim 1.

Claims 14 and 17 each recite the limitation "at least one bit input to the randomizing operation is transmitted to the next randomizing operation via at least two paths". Similarly, **Claims 15 and 18** each recite the limitation "at least one bit input to the randomizing operation is transmitted to the next randomizing operation via at least two randomizing and diffusing paths". It is not clear how the same bit can be transmitted by two different paths, as this contradicts the specification; namely, the specification states that at the intersections of the paths depicted in, for example, Figure 35, the bits carried on the lines are exclusive ORed (see page 51, lines 2-5, of the present specification). Because the bits are combined with other bits, the exact same bit information is not transmitted by the different paths; however, the claim language

suggests that a bit, unchanged, is transmitted between the randomizing operations. This contradiction renders the claims indefinite.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

12. Claims 1, 4-6, 8, 9, 11, and 14-18 are rejected under 35 U.S.C. 102(b) as being anticipated by Delayaye et al, US Patent 4751733.

In reference to Claim 1, Delayaye discloses an apparatus for block encryption that includes a series of encrypting sections, each of which includes a unit to randomize subblock data obtained by dividing block data and a unit to diffuse data output from the randomizing unit (see Figure 1, permutation circuits 1, 6, and 8, and substitution memories 2-5, and Figures 5 and 6 for examples of substitution memories providing input to several succeeding units through the diffusing/permutation circuits).

In reference to Claim 4-6, Delayaye discloses an apparatus for block encryption that includes a series of encrypting sections, each of which includes a first nonlinear

transformation unit and a first linear diffusion unit (see Figure 1, permutation circuits 1, 6, and 8, and substitution memories 2-5, and Figures 5 and 6 for examples of substitution memories providing input to several succeeding units through the diffusing/permutation circuits). Delayaye further discloses that the first nonlinear transformation unit can include a second nonlinear transformation unit and a second linear diffusion unit (note that there are multiple permutation and substitution circuits in Figure 1; see also column 8, lines 12-37, particularly noting that it is possible to perform any number of possibly asymmetrical successions of substitution-permutations).

In reference to Claim 8, Delayaye further discloses that the blocks can be 128 bits in length with subblocks of 32 bits (column 2, lines 20-32, where a block size of 32 bits is easily increased, noting that four 32 bit blocks results in a 128 bit block).

In reference to Claims 9 and 11, Delayaye further discloses implementing the diffusion unit in hardware (note the memories in Figure 1) or software (the memories may be programmable, column 5, lines 54-56).

Claims 14 and 15 are directed to a method and a software implementation, respectively, of the apparatus of Claim 1, and are rejected by a similar rationale.

Claim 16 is directed to a decryption apparatus which merely performs the reverse function of the encryption apparatus of Claim 1, and is rejected by a similar rationale, further noting that Delayaye discloses that the same device may be used for enciphering and deciphering (column 3, lines 42-46). Claims 17 and 18 are directed to

a method and a software implementation, respectively, of the apparatus of Claim 16, and are rejected by a similar rationale.

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 10, 12, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Delayaye in view of Matsui et al, US Patent 6201869.

In reference to Claim 10, Delayaye discloses everything as applied to Claim 9 above. However, Delayaye does not explicitly disclose that the diffusion unit is based on multiplication over a Galois field. Matsui discloses a block encryption apparatus that includes a diffusion unit based on operations over a Galois field (see, for example, column 8, lines 45-48). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Delayaye by basing the diffusion unit on operations over a Galois field, in order to increase the speed of encryption (see Matsui, column 2, lines 4-8).

In reference to Claims 12 and 13, Delayaye discloses an apparatus for block encryption that includes a series of encrypting sections, each of which includes first

nonlinear transformation unit and a first diffusion unit (see Figure 1, permutation circuits 1, 6, and 8, and substitution memories 2-5, and Figures 5 and 6 for examples of substitution memories providing input to several succeeding units through the diffusing/permutation circuits). Delayaye further discloses that the first nonlinear transformation unit can include a second nonlinear transformation unit and a second linear diffusion unit (note that there are multiple permutation and substitution circuits in Figure 1; see also column 8, lines 12-37, particularly noting that it is possible to perform any number of possibly asymmetrical successions of substitution-permutations, and further noting that the orders of operations can be changed and that operations can be carried out in several steps). Although Delayaye does not explicitly disclose the block sizes of 128 or 64 bits of Claims 12 and 13 respectively, Delayaye states that the block size may be changed (column 2, lines 20-32). Further, although Delayaye does disclose using the key in the substitution boxes (see Figure 1), Delayaye does not explicitly disclose key addition units. Delayaye also does not explicitly disclose the use of an operation based on multiplication over a Galois field.

Matsui discloses a block encryption apparatus that includes a diffusion unit based on operations over a Galois field (see, for example, column 8, lines 45-48). Matsui further discloses the use of key addition units (the key is used at the XOR circuits, column 8, lines 45-48). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Delayaye by basing the diffusion unit on operations over a Galois field and including the

key addition units, in order to increase the speed of encryption (see Matsui, column 2, lines 4-8).

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Feistel, US Patent 3798359, discloses a substitution permutation block cipher cryptographic system, where the outputs of subblocks are sent by multiple paths to subsequent processing blocks (see, for example, Figures 7 and 8).

b. Davida et al, US Patent 4275265, discloses a substitution permutation ciphering circuit that includes diffusion between substitution blocks along multiple paths (see, for example, Figure 1).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

3710
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER